UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,515	07/25/2003	Lee E. Cannon	29757/P-834	3255

4743 7590 02/08/2007

MARSHALL, GERSTEIN & BORUN LLP
233 S. WACKER DRIVE, SUITE 6300
SEARS TOWER
CHICAGO, IL 60606

EXAMINER	
THOMASSON, MEAGAN J	
ART UNIT	PAPER NUMBER
3714	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/627,515	CANNON, LEE E.	
	Examiner	Art Unit	
	Meagan Thomasson	3714	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 August 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) *37 and 41* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36,38-40 and 42-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

The examiner acknowledges the amendments made to claims 19,26,32-34 and 38. Claims 37 and 41 have been canceled.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-36,38-40, and 42-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Martinek et al. (WO 03/045519), "Martinek" in view of Rackman (US 4,670,857), "Rackman".

Claims 1, 19, 32, 38, 39, 42 and 46: Martinek discloses an apparatus:

- a display unit(pg. 24, line 27);
- a value input device(pg. 24, line 27);
- a controller operatively coupled to said display unit and said value input device, said controller comprising a processor and a memory operatively coupled to said processor (pg. 25, lines 10, 11 and lines 27-31),
- said controller being programmed to receive downloadable gaming data from a data storage device external to said gaming apparatus(pg. 27, lines 11-19);

- said controller being programmed to receive encrypted gaming data from said data storage device, said encrypted gaming data having been generated by performing a hash function on gaming data to form a first message digest and by encrypting said first message digest utilizing a private encryption key of a gaming data authoring organization and a private encryption key of a gaming regulatory organization(pg. 27, line 13 – pg. 28, line 7);

- said controller being programmed to decrypt said encrypted gaming data utilizing a public encryption key of said gaming data authoring organization and a public encryption key of said gaming regulatory organization to form a decrypted message digest(pg. 29, lines 21-25);

- said controller being programmed to perform a hash function on said downloadable gaming data to generate a second message digest(pg. 27, lines 30-33 and pg. 30, lines 18-25); and

- said controller being programmed to compare said decrypted message digest with said second message digest to determine if said downloadable gaming data is authorized(pg. 27, line 30-33 and pg. 30, lines 18-25).

Martinek does not disclose double encryption as claimed. Instead, Martinek teaches single encryption (pg. 27, line 13 – pg. 28, line 7) and authentication from both a regulatory agency (pg. 30, lines 26-28) and a game code manufacturer (pg. 31, lines 1-2). In an analogous game security reference, Rackman (col. 6, lines 1-13) teaches doubly encrypting the message to insure both privacy and authentication.

One of ordinary skill in the art would have seen the benefit of double encryption because it allows the receiver to authenticate the transmitter and the transmitter to allow only the receiver to decrypt the message. Therefore, it would have been obvious to one or ordinary skill in the art at the time of the instant invention to modify Martinek with double encryption as taught by Rackman to insure both privacy and authentication.

Claim 2: Martinek discloses an apparatus wherein said data storage device comprises a portable data storage medium on which said downloadable data was stored when said portable data storage medium was at a location external to said gaming apparatus and wherein said portable data storage medium is physically moved so that it is operatively coupled to said gaming apparatus in order to transfer said downloadable gaming data to said controller (pg. 26, lines 19-30).

Claims 3, 21, 44, and 48: Martinek discloses an apparatus wherein-said controller is programmed to receive downloadable gaming data that comprises substantially all gaming data that is necessary to facilitate play of a casino game (pg. 26, lines 15-18).

Claims 4, 22, 33, 40, and 41: Martinek does not disclose an apparatus wherein said controller is programmed to receive from said data storage device encrypted gaming data that was generated by triply encrypting said first message digest utilizing said private encryption key of said gaming data authoring organization, said private encryption key of said gaming regulatory organization, and a private encryption key of a

casino, and wherein said controller is programmed to triply decrypt said encrypted gaming data utilizing said public encryption key of said gaming data authoring organization, said public encryption key of said gaming regulatory organization, and a public encryption key of said casino to form said decrypted message digest.

Instead, Martinek teaches single encryption (pg. 27, line 13 – pg. 28, line 7) and authentication from a regulatory agency (pg. 30, lines 26-28), a game code manufacturer (pg. 31, lines 1-2) and casinos (pg. 3, lines 24-33). In an analogous game authentication reference, Rackman teaches doubly encrypting the message to insure both privacy and authentication (col. 6, lines 1-13). It would have been obvious to one of ordinary skill in the art to add a third encryption to increase the layers of encryption and therefore increase security. One would have seen the benefit of the third layer of encryption supported by the casino, game regulatory authority and/or game code manufacturers because casino management and the governmental regulatory agencies are very concerned with electronic intruders tapping into the casino communication network and manipulating any player terminal, including a slot machine, to fraudulently declare a jackpot. Therefore, it would have been obvious to one or ordinary skill in the art at the time of the instant invention to modify Martinek as modified by Rackman with a third encryption to provide casinos and regulatory agencies (and game code manufacturers) to insure privacy and authentication; thereby preventing tampering and fraudulent jackpots.

Claim 5: Martinek discloses an apparatus wherein said gaming system additionally comprises a central computer operatively coupled to each of said gaming apparatuses,

said central computer comprising a memory, and wherein said controller is programmed to receive said downloadable gaming data from said memory of said central computer (pg. 11, lines 21-33).

Claims 6, 26, and 34: Martinek discloses an apparatus, comprising:

- a display unit (pg. 24, line 27);
- a value input device (pg. 24, line 27);
- a controller operatively coupled to said display unit and said value input device, said controller comprising a processor and a memory operatively coupled to said processor, said controller being programmed to receive downloadable gaming data from a data storage device external to said gaming apparatus(pg. 25, lines 10, 11 and lines 27-31);
- said controller being programmed to receive encrypted gaming data from said data storage device, said encrypted gaming data having been generated by performing a data-abbreviating function on gaming data to form first abbreviated gaming data and by doubly encrypting said first abbreviated gaming data utilizing an encryption key of a gaming data authoring organization and an encryption key of a gaming regulatory organization (pg. 8, lines 13-27);
- said controller being programmed to decrypt said encrypted gaming data utilizing an encryption key of said gaming data authoring organization and an encryption

key of said gaming regulatory organization to form decrypted gaming data(pg. 27, line 13 – pg. 28, line 7);

- said controller being programmed to perform a data-abbreviating function on said downloadable gaming data to generate second abbreviated gaming data(pg. 8, lines 13-27); and
- said controller being programmed to compare said decrypted gaming data with said second abbreviated gaming data to determine if said downloadable gaming data is authorized(pg. 8, lines 13-27).

Martinek does not disclose double encryption as claimed. Instead, Martinek teaches single encryption (pg. 27, line 13 – pg. 28, line 7). In an analogous game security reference, Rackman (col. 6, lines 1-13) teaches doubly encrypting the message to insure both privacy and authentication. One of ordinary skill in the art would have seen the benefit of double encryption because it allows the receiver to authenticate the transmitter and the transmitter to allow only the receiver to decrypt the message. Therefore, it would have been obvious to one or ordinary skill in the art at the time of the instant invention to modify Martinek with double encryption as taught by Rackman to insure both privacy and authentication.

Claims 7: Martinek discloses an apparatus wherein said controller is programmed to receive encrypted gaming data that was generated by first encrypting said first

abbreviated gaming data utilizing said encryption key of said gaming data authoring organization to form singly encrypted gaming data and then encrypting said singly encrypted gaming data with said encryption key of said gaming regulatory organization (pg. 30, lines 26-30).

Claim 8: Martinek discloses an apparatus wherein said controller is programmed to first decrypt said encrypted gaming data utilizing said encryption key of said gaming data authoring organization to form singly encrypted gaming data and then to decrypt said singly encrypted gaming data utilizing said encryption key of said gaming regulatory organization (pg. 30, lines 26-30).

Claims 9, 28, 35, 36: Martinek discloses an apparatus wherein said data storage device comprises a computer located at a location remote from said gaming apparatus and wherein said controller is programmed to receive said downloadable gaming data from said computer (pg. 11, lines 21-33).

Claims 10, 29: Martinek discloses an apparatus wherein said data storage device comprises a portable data storage medium on which said downloadable data was stored when said portable data storage medium was at a location external to said gaming apparatus and wherein said portable data storage medium is physically moved so that it is operatively coupled to said gaming apparatus in order to transfer said downloadable gaming data to said controller(pg. 26, lines 19-30).

Claims 11, 30: Martinek discloses an apparatus wherein said controller is programmed to receive said encrypted gaming data along with said downloadable gaming data(pg. 27-29).

Claim 12: Martinek discloses an apparatus wherein said controller is programmed to receive downloadable gaming data that comprises substantially all gaming data necessary to facilitate play of a casino game(pg. 26, lines 15-18).

Claims 13, 31: Martinek discloses an apparatus wherein said controller is programmed to receive said encryption key of said gaming data authoring organization and said encryption key of said gaming regulatory organization(pg. 30, lines 26-30).

Claims 14, 32 and 33: Martinek does not disclose an apparatus wherein said controller is programmed to receive from said data storage device encrypted gaming data that was generated by triply encrypting said first abbreviated gaming data utilizing said encryption key of said gaming data authoring organization, said encryption key of said gaming regulatory organization, and an encryption key of a casino, and wherein said controller is programmed to triply decrypt said encrypted gaming data utilizing an encryption key of said gaming data authoring organization, an encryption key of said gaming regulatory organization, and an encryption key of said casino to form said decrypted data product.

Instead, Martinek teaches single encryption (pg. 27, line 13 – pg. 28, line 7) and authentication from a regulatory agency (pg. 30, lines 26-28), a game code manufacturer (pg. 31, lines 1-2) and casinos (pg. 3, lines 24-33). In an analogous game

authentication reference, Rackman teaches doubly encrypting the message to insure both privacy and authentication (col. 6, lines 1-13). It would have been obvious to one of ordinary skill in the art to add a third encryption to increase the layers of encryption and therefore increase security. One would have seen the benefit of the third layer of encryption supported by the casino, game regulatory authority and/or game code manufacturers because casino management and the governmental regulatory agencies are very concerned with electronic intruders tapping into the casino communication network and manipulating any player terminal, including a slot machine, to fraudulently declare a jackpot. Therefore, it would have been obvious to one or ordinary skill in the art at the time of the instant invention to modify Martinek as modified by Rackman with a third encryption to provide casinos and regulatory agencies (and game code manufacturers) to insure privacy and authentication; thereby preventing tampering and fraudulent jackpots.

Claim 15: Martinek discloses an apparatus wherein said display unit comprises a video display unit that is capable of generating video images (pg. 24, line 27).

Claims 16, 27: Martinek discloses an apparatus wherein said controller is programmed to cause a video image comprising an image of at least five playing cards to be displayed if said game comprises video poker, wherein said controller is programmed to cause a video image comprising an image of a plurality of simulated slot machine reels to be displayed if said game comprises video slots, wherein said controller is programmed to cause a video image comprising an image of a plurality of playing cards to be displayed if said game comprises video blackjack, wherein said controller is

programmed to cause a video image comprising an image of a plurality of keno numbers to be displayed if said game comprises video keno, wherein said controller is programmed to cause a video image comprising an image of a bingo grid to be displayed if said game comprises video bingo (pg. 2, lines 13-30 and pg. 34, lines 23-33).

Claim 17: Martinek discloses an apparatus wherein said display unit comprises at least one mechanical slot machine reel(pg. 34, line 28).

Claim 18: Martinek discloses an apparatus wherein said gaming system additionally comprises a central computer operatively coupled to each of said gaming apparatuses, said central computer comprising a memory, and wherein said controller is programmed to receive said downloadable gaming data from said memory of said central computer(pg. 11, lines 21-33).

Claim 20: Martinek discloses an apparatus wherein said controller is programmed to cause, if said first gaming data is authorized, said display unit to generate a game display representing one of the following games: poker, blackjack, slots, keno or bingo (pg. 2, lines 13-30 and pg. 34, lines 23-33).

Claims 23, 45: Martinek discloses an apparatus wherein said display unit comprises a video display unit that is capable of generating video images(pg. 24, line 27).

Claims 24, 43, 47: Martinek discloses an apparatus, wherein said controller is programmed to cause a video image comprising an image of at least five playing cards to be displayed if said game comprises video poker, wherein said controller is

programmed to cause a video image comprising an image of a plurality of simulated slot machine reels to be displayed if said game comprises video slots, wherein said controller is programmed to cause a video image comprising an image of a plurality of playing cards to be displayed if said game comprises video blackjack, wherein said controller is programmed to cause a video image comprising an image of a plurality of keno numbers to be displayed if said game comprises video keno, wherein said controller is programmed to cause a video image comprising an image of a bingo grid to be displayed if said game comprises video bingo(pg. 2, lines 13-30 and pg. 34, lines 23-33).

Claim 25: Martinek discloses an apparatus wherein said display unit comprises at least one mechanical slot machine reel(pg. 34, line 28).

Response to Arguments

Applicant's arguments filed August 16, 2006 have been fully considered but they are not persuasive.

Regarding claim 1, applicant argues that the limitation of generating encrypted game data by means of performing a hash function to form a first message digest, and then doubly encrypting said first message digest utilizing a private encryption key of a gaming data authoring organization and a private encryption key of a gaming regulatory organization, is not met by neither Martinek nor Rackman, has been considered but is not persuasive. In contrast to the statement made on page 14, 5th paragraph of applicant's remarks that "the Office Action alleges that Rackman teaches double

encryption as claimed", the Office Action of May 16, 2006 alleges that Martinek taken in combination with Rackman teaches the claimed method of double encryption.

Martinek discloses creating a message digest by hashing a data set. The message digest is encrypted utilizing a private key algorithm where it is then stored on an external data storage device (Martinek p. 28, line 30 – p. 29, line 4). Martinek discloses that the digital signature, or key, that may be utilized for purposes of encryption may be that of a gaming regulatory agency (p. 30, lines 26-27). In addition, Martinek discloses that the digital signature, or key, that may be utilized for purposes of encryption may be that of a gaming data authoring organization (p. 29, line 33 - p.30, line 2). Martinek does not disclose utilizing the encryption key of the gaming regulatory agency in combination with that of the gaming data authoring organization to form a doubly encrypted data set. However, Rackman contemplates providing additional insurance for privacy and authentication by doubly encrypting a data set, that is, encryption of a data set through the use to two separate keys. Thus, the combination of Martinek and Rackman teach the limitation of doubly encrypting a first message digest utilizing two separate keys, wherein the first of said keys may be from a gaming regulatory agency, and the second of said keys may be from a data authoring organization. The decryption process is also disclosed, wherein upon receipt of an encrypted data set, the recipient, i.e. the gaming terminal, utilizes a public decryption key to form a decrypted message digest as well as performing a hash function on said data set to generate a second message digest; and then comparing said decrypted message digest with said second message digest to determine if the data set is

authorized (p. 23, lines 22-25; Fig. 4). Because Rackman teaches the limitation of double encrypting a first message digest utilizing two separate keys, the decryption process resultant from the combination of Martinek and Rackman would similarly require the use of two keys, which, as disclosed by Martinek, may be that of a gaming regulatory agency and/or that of a data authoring organization.

Regarding claim 34, applicant's argument that Martinek in combination with Rackman do not disclose, teach, or suggest the limitation of "causing said gaming data and said doubly encrypted abbreviated gaming data to be transferred to a controller" has been considered but is not persuasive. In addition to the encryption/decryption method as described above, Martinek additionally discloses abbreviating a gaming data set, encrypting said abbreviated data set, and then storing the data set for future transfer to a gaming machine controller (p. 8, lines 24-28).

Regarding claims 42 and 46, applicant argues that Martinek in combination with Rackman does not disclose, teach, or suggest the limitation of having a first encrypted gaming data stored in memory and a second encrypted gaming data stored in memory, said first encrypted gaming data having been generated by encrypting gaming data utilizing an encryption key of a first gaming organization and said second encrypted gaming data having been generated by encrypting gaming data utilizing an encryption key of a second gaming organization; in addition, a controller being programmed to retrieve the first and second data sets, decrypt them in accordance with the keys associated with their respective gaming organizations, and then determine if the decrypted gaming data sets are identical. The invention disclosed by the combination of

Martinek and Rackman is capable of receiving and decrypting gaming data sets from any gaming organization for which it possesses a public key, and therefore would be capable of receiving and decrypting multiple gaming data sets. Regarding the limitation that the two data sets are then compared to determine if they are identical, the invention disclosed by Martinek in combination with Rackman teaches comparison of decrypted data sets (Fig. 4), and would therefore have been capable of decrypted and comparing any received data sets, including those received from two separate gaming organizations.

Regarding claims 32 and 33, applicant's argument that the limitation of "triply decrypting said encrypted gaming data utilizing a first encryption key, a second encryption key, and a third encryption key, each of said encryption keys being different", and further that the three keys may represent a casino, a public gaming data authoring organization, and a public gaming regulatory organization, is not persuasive. Martinek discloses singly encrypted data utilizing keys from any of a game server of a game host or casino (p. 3, lines 25-33), a gaming data authoring organization (p. 29, line 33 - p.30, line 2), or a gaming regulatory organization (p. 30, lines 26-30). Rackman discloses doubly encrypting data utilizing two separate keys, as described above. The argument that the three key usage is novel in its ability to allow authentication of multiple parties by the receiver is not persuasive, as the combination of Martinek and Rackman could also perform the same function; that is, the receiver, i.e. gaming console, could authenticate data received from the plurality of organizations to whom the keys belong. The notion that the data set may be encrypted multiple times to provide an added

degree of privacy and security was presented in Rackman. In light of this, to increase the number of times that the data is encrypted would have been obvious to one of ordinary skill in the art.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Meagan Thomasson whose telephone number is (571) 272-2080. The examiner can normally be reached on M-F 830-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bob Olszewski can be reached on (571) 272-6788. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Meagan Thomasson
February 5, 2007

2/5/07

ROBERT OLSZEWSKI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3700